ESA/SMA SAML SSOの自己署名証明書の生成と設定

内容

はじめに

このドキュメントでは、Security Assertion Markup Language(SAML)サービスプロバイダー(SP)設定用の自己署名証明書(SSC)を作成する方法について説明します。

前提条件

このドキュメントを使用して、Eメールセキュリティアプライアンス(ESA)およびセキュリティ管理アプライアンス(SMA)上のSecurity Assertion Markup Language(SAML)2.0シングルサインオン(SSO)サービスプロバイダー(SP)設定用の自己署名証明書を生成します。

要件

方法1(ESA Web UI):Web UIでのESA管理アクセスおよび証明書を管理する権限。

方法2（OpenSSLコマンド）:OpenSSLがインストールされ、コマンドラインから使用できる。

Windows:OpenSSLをインストールします。

macOS、Linux、またはUnix:OpenSSLは通常、デフォルトで、またはオペレーティングシステム

パッケージマネージャから使用できます。

使用するコンポーネント

特定のハードウェアおよびソフトウェア要件はありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報

このドキュメントは、Security Assertion Markup Language(SAML)2.0シングルサインオン(SSO)を使用するEメールセキュリティアプライアンス(ESA)およびセキュリティ管理アプライアンス(SMA)の導入に適用されます。 SAML SP構成では、サービスプロバイダーのセットアップにSecure Sockets Layer(SSL)証明書が必要です。 証明書は、内部の証明書ツール、認証局(CA)、または自己署名証明書から取得できます。

問題

自己署名証明書は、ESAおよびSMA用の一部のSAML SP環境で必要です。このドキュメントでは、証明書と秘密キーを作成し、オプションで秘密キーをパスフレーズで暗号化する方法について説明します。

解決策

- Windowsの場合、Windows用のOpenSSLをインストールします。この方法については、オンラインのチュートリアルを参照してください。
- Unix、macOS、およびLinuxでは、通常OpenSSLはデフォルトで使用できます。
- ESAがすでに証明書を管理しており、SAML SPで使用するために証明書を工クスポートする必要がある場合は、ESA Web UI方式を使用します。
- 証明書とキーペアをコマンドラインから直接作成する必要がある場合は、OpenSSLコマンドメソッドを使用します。

方法1:ESA Web UIで自己署名証明書を作成およびエクスポートする

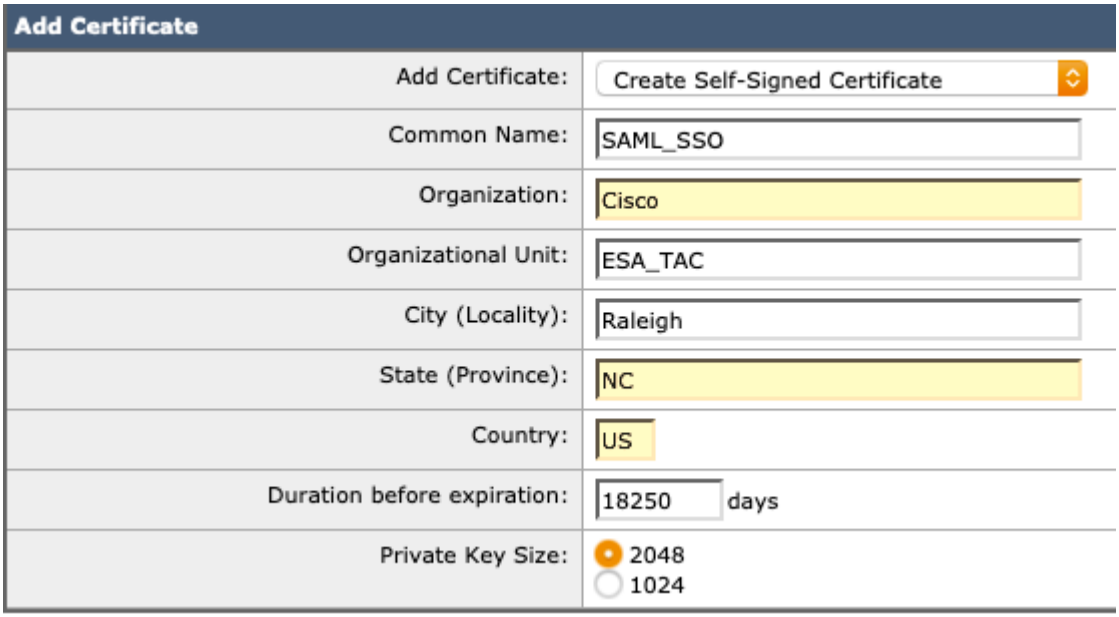
ESAがすでに証明書を管理しており、SAML SPで使用するために証明書をエクスポートする必要がある場合は、この方法を使用します。

証明書を作成します。

1. ESA Web UIで、Network > Certificatesに移動します。Add Certificateを選択し、次にCreate Self-Signed Certificateを選択します。

2. テンプレート· フィールドに、共通名、組織、組織単位、市、州、国および期間(1-18250日)を入力します。

3. 秘密キーのサイズを2048に設定します。



完全な自己署名証明書テンプレート

4. 証明書を発行し、結果を確認して、Commit Changesを選択します。

Certificate Name:	SAML_SSO
Common Name:	SAML_SSO
Organization:	Cisco
Organization Unit:	ESA_TAC
City (Locality):	Raleigh
State (Province):	NC
Country:	US
Signature Issued By:	Common Name (CN): SAML_SSO Organization (O): Cisco Organizational Unit (OU): ESA_TAC Issued On: Sep 20 15:50:27 2019 GMT Expires On: Sep 7 15:50:27 2069 GMT

設定後の表示

証明書をエクスポートします。

1. ESA Web UIで、Network > Certificates > Export Certificateの順に移動します。

2. エクスポートする証明書を選択し、パスフレーズを作成します。次に、Exportを選択し、ファイルをディレクトリに保存します。

注：管理用SAML SSOは、PKCS#12(PFX)証明書をインポートできます。秘密キーの暗号化が不要な場合、残りの変換手順はオプションです。

証明書を変換します。

エクスポートされた証明書はPKCS#12/PFX形式であり、プライバシー強化メール(PEM)への変換が必要です。

次のOpenSSLコマンドを実行して、PFXファイルをPEM形式に変換します。

<#root>

openssl

```
 pkcs12 -in <certname>.pfx -nokeys -out cert.pem -nodes
```

<#root>

openssl

```
 pkcs12 -in SAML_SSO.pfx -out UNIX_FULL.pem -nodes
```

内容を編集し、出力を2つのファイルに分割します。

1. 新しく変換されたファイルを編集する必要があります。

2. テキストエディタで2つの空のファイルを開き、<name>.crtと<name>.keyという名前を付けます。

3. 変換されたファイルから-----BEGIN CERTIFICATE----- ~ -----END CERTIFICATE-----のセクションをコピーします。

4. 内容を<name>.crtファイルに貼り付けて保存します。

5. 変換されたファイルから-----BEGIN PRIVATE KEY----- ~ -----END PRIVATE KEY-----のセクションをコピーします。

6. 内容を<name>.keyファイルに貼り付けて保存します。

7. これで、証明書とキーを構成のSAML SP部分にロードできます。

方法2:OpenSSLコマンドを使用して自己署名証明書とキーペアを作成する

この方法は、証明書とキーペアをコマンドラインから直接作成する必要がある場合に使用します。

証明書と鍵のペアを作成します。

Unix、Linux、またはmacOSのコマンドラインインターフェイス(CLI)でOpenSSLコマンドを実行します。domainを必要な名前で置き換えます。

<#root>

openssl

```
 req -newkey rsa:2048 -nodes -keyout domain.key -x509 -days 1095 -out domain.crt
```

作成時に、リストされているフィールドのプロンプトが表示されます。

コマンドが実行されるディレクトリに、saml_ssl.crtとsaml_ssl.keyの2つのファイルが生成されます。

```
$ openssl req -newkey rsa:2048 -nodes -keyout saml_sso.key -x509 -days 1095 -out saml_sso.crt
Generating a 2048 bit RSA private key
..........+++
.....................................................................................................
writing new private key to 'saml_sso.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:NC
Locality Name (for example, city) []:Raleigh
Organization Name (for example, company) []:Cisco
Organizational Unit Name (for example, section) []:ESA_TAC
Common Name (for example, fully qualified host name) []:SAML_SSO
Email Address []:user@example.com
```

秘密キーを暗号化します (オプション。設定には不要) 。

注：パスフレーズの例は再利用しないでください。このキーは単なる例です。

次のOpenSSLコマンドは、暗号化されていない秘密キー(unencrypted.key)を取得し、暗号化されたキー(encrypted.key)を出力します。

<#root>

openssl

```
 rsa -des3 -in unencrypted.key -out encrypted.key
```

<#root>

openssl

```
 rsa -des3 -in saml_sso.key -out saml_secure.key
```

```
$ openssl rsa -des3 -in saml_sso.key -out saml_secure.key
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

```
$ ls

saml_sso.crt
saml_sso.key
saml_secure.key
```

証明書とキーは、SAML SSO SPまたはSpam SSO SPのセットアップの準備が整っています。

関連情報

Cisco E メール セキュリティ アプライアンス：エンドユーザ ガイド

Ciscoコンテンツセキュリティ管理アプライアンス – エンドユーザガイド

Cisco Webセキュリティ：エンドユーザガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。